Department of Health
Policy/Procedure

Number:	17.005
Title:	Employee Responsibilities with Confidential Information
References:	RCW 42.17, RCW 42.48, RCW 9A.20.21, WAC 356-34-010, DOH Policy/Procedures 02.001, 07.010, 17.003
Contact:	Assistant Secretary, Management Services Division
Effective Date: June 1, 1999	
Supersedes:	N/A
Approved: Signed by Mary C. Selecky	
	Secretary, Department of Health

Policy Statement:

All records of the Department of Health (DOH) are public records and are publicly disclosable except those exempt under RCW 42.17 and other applicable laws per DOH Policy 17.003.

To maintain the public's trust and achieve its mission, the department must act as a responsible custodian of the information it holds. It must protect the privacy of individuals and other entities and ensure that confidential information is protected from inadvertent or intentional misuse and disclosure, while allowing for records that are publicly disclosable to be made available to the public. It must also ensure the data/information it holds are as accurate as possible, available for use by those who need it, and are not subject to tampering, fraud, or loss.

Public disclosure laws require agencies to make governmental records, with some exceptions, available to the public. However, confidential data/information in any form where the individual may be identified is not to be disclosed, except as allowed by law. In most cases, records can be disclosed when data/information that identifies or may reasonably lead to the identification of an individual are removed. The process for disclosure is documented in DOH Policy 17.003.

Access to identifiable and confidential data/information will be limited to DOH staff and others who are authorized to use the data/information to achieve the authorized purposes of a DOH project or program. Use by other personnel or for other purposes (e.g., research) will require written approval from the division's Assistant Secretary, or designee per DOH Policy/Procedure 02.001, and will only be granted in accordance with law.

Confidentiality practices and security protections will be monitored throughout DOH on an ongoing basis. Suspected confidentiality breaches will be thoroughly investigated.

This policy is intended to protect the citizens whose information has been entrusted to the state, as well as DOH and DOH staff as each act in good faith in handling confidential data/information.

Purpose:

This policy outlines the general responsibilities that govern DOH and its staff around the collection, transmission, storage, maintenance, destruction, analysis, and release of identifiable and confidential data/information held by DOH. It describes a common framework to develop minimum practices to be followed by all department staff to ensure confidentiality and security of all data/information held by DOH. Individual programs may set more stringent requirements as needed or mandated, but at a minimum must follow these practices. This policy applies to all DOH staff, contractors, volunteers, students/interns, and federal assignees who could potentially come into contact with confidential data/information held by DOH. Contact might occur through the collection, transmission, storage, maintenance, destruction, analysis, and distribution of data/information, received or sent through telephone communications, electronic mail, faxes, and paper records.

This policy applies to all data and information held by DOH regardless of subject matter, source, or format. The latter includes, but is not limited to, paper (such as reports, letters, and memos), electronic computer files (stored on hard drives, diskettes, CD-ROM, tapes, or other media), electronic mail, and faxes. The policy covers backups and data extracts as well as original data/information held by DOH.

Definitions:

Confidentiality - pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged in identifiable form. Exceptions can be made in limited circumstances for disclosure to others in ways as specified in law. Confidential treatment includes mandating specific controls over data/information such as monitoring and strictly limiting access to and disclosure of the data/information.

Confidentiality breach - an unauthorized release of identifiable or confidential data/information, which may result from a security failure, intentional inappropriate behavior, human error, or natural disaster. A breach of confidentiality may or may not result in harm to one or more individuals.

Identifiable data/information - personal data/information that identifies, or is reasonably likely to be used to identify, an individual. Identifiable data/information may include, but is not limited to, name, address, telephone number, social security number, and medical record number. Data elements that may identify an individual can vary depending on the geographic location and other variables (e.g., rarity of person's health condition or patient characteristics). Linkage of databases and use of Geographic Information Systems (GIS) enhance the ability to identify individuals from limited amounts of information. These uses of data/information must be considered when determining what elements in a database may be identifiable. For the purposes of this policy, "identifiable information" will include potentially identifiable information.

Public Record - includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. [RCW 42.17.020 (36)]

Writing - means handwriting, typewriting, printing, Photostatting, photographing, and every other means of recording any form of communication or representation, including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated. [RCW 42.17.020 (42)]

DOH Confidentiality Procedures:

DOH will be responsible for confidentiality and security training in conjunction with this policy. DOH will make every effort to assure that physical security of confidential data/information is protected. DOH will develop a common framework for division specific confidential data identification for use in developing division specific confidentiality procedures.

Each division will also determine the proper procedures for the handling of confidential information. The division should use current laws, regulations, and federal requirements as well as guidance documents developed by DOH for the handling of confidential information in making this determination. Each division will be responsible for assuring training on division specific confidentiality procedures will occur.

Each office or program will determine what data/information originating or maintained in that office are identifiable and confidential. Determinations, to be finalized by the office/program manager, will be based on law and regulation after consultation with staff and other advising entities. This determination will be documented and shared, where it can be consistently defined, with the Office of Information Resource Management (OIRM) Information Resource Directory Administrator and any entities who are allowed/granted access to the data/information. Any potentially identifiable or confidential data/information within DOH will not be shared until the program that originated or maintains the data are consulted.

Each employee will read and sign that they understand their responsibilities under this policy. For employees with DOH as of June 1, 1999, this requirement is effective on June 1, 2000 and should occur either as part of the next scheduled annual employee evaluation or in conjunction with DOH confidentiality and security training. For employees hired after June 1, 1999, this requirement is effective on the first day of employment with DOH.

Penalties

The agency will take appropriate measures to protect the integrity and confidentiality of data/information under its jurisdiction. Investigations will determine if a confidentiality breach constitutes a violation of this policy. Violations of this policy may be subject to civil and/or criminal penalties:

1) Willful violation of DOH rules or regulations can result in a disciplinary action to demote, suspend, reduce in salary, or dismiss an employee. [WAC 356-34-010(1)] Disciplinary actions taken against an employee may be appealed according to DOH Policy 7.010.

2) Unauthorized use or disclosure of confidential data/information may be considered an ethics violation and subject to civil damages or other penalties.

3) If an unauthorized disclosure results from a research project approved by an agency research review board, DOH staff involved in the project may be liable under RCW 42.48 (Release of Records for Research). The violation is a gross misdemeanor subject to imprisonment of not more than one year and/or a fine, in an amount not more than five thousand dollars. [RCW 42.48.050 and 9A.20.021]

4) Specific sources of confidential data and information, such as information related to HIV/STD conditions, mental health, and drug and alcohol abuse treatment, may be subject to stricter state and federal penalties.

Responsibilities:

Responsibility	Action
Assistant Secretary, Management Services Division	Assure ongoing DOH confidentiality and security training. Assure that training, policy, and acknowledgement remain current. Represent department in civil or criminal proceedings against an employee or DOH related to violation of confidentiality statutes. Provide oversight to DOH confidentiality policies and procedures. Lead investigations of potential violations of this policy/procedure.
Assistant Secretary	Assure division staff have ready access to DOH confidentiality policies/procedures and adequate and timely training on these policies and procedures. Develop division specific confidentiality procedures. Assure that division office and program managers have determined which data/information originating or maintained in the office or program is confidential. As allowable by law, approve or disapprove use of identifiable and confidential data/information originating or maintained in their division for purposes other than for clearly authorized DOH program/projects. Determine appropriate disciplinary action for violations of this policy/procedure by staff in their division.
Office/Program Manager/ Supervisor	Assure that office-specific confidentiality policies/procedures and regulations are in place. Based on existing laws and regulations and after consultation with staff and other advising entities, determine which data elements/information in databases originating or maintained in their office/program are confidential. Provide list of database elements/information that are confidential to OIRM Information Resource Directory Administrator where appropriate. Assure office/program staff have ready access to DOH and division confidentiality policies/procedures and adequate and timely training on these policies and procedures. Assign employees to DOH confidentiality and security training. Provide training to employees in their office/program regarding the appropriate use and handling of program specific confidential data/information following division procedures. Identify which staff needs access to identifiable and

	confidential data/information for the purposes of authorized DOH programs/projects. Assure employee reads, understands, and acknowledges DOH and division specific confidentiality policies and procedures upon initial employment and in conjunction with the annual employee evaluation. Assure original, signed confidentiality acknowledgments are forwarded to the Human Resources Office for inclusion in the employee's personnel file. Assure that DOH originated or maintained confidential data/information is not inappropriately retained by the employee and is returned to the program upon termination of employment or transfer to another position in DOH.
Employee	Read and understand DOH and division confidentiality policies and procedures and sign the confidentiality acknowledgment upon initial employment (computer user ID will not be issued until confidentiality acknowledgment is signed), and as part of the annual employee evaluation. Participate in agency and division specific confidentiality training as assigned by their supervisor. Not engage in unauthorized release, access to, or modification of identifiable, confidential, or other DOH data/information. Report any suspected confidentiality breach to the supervisor. Assure that DOH originated or maintained confidential data/information is not inappropriately retained by the employee and is returned to the program upon termination of employment or transfer to another position in DOH.
DOH contractors, volunteers, students/interns, federal assignees	Sign DOH confidentiality acknowledgment. Participate in DOH and/or division specific confidentiality and security training as appropriate. Not engage in unauthorized release, access to, or modification of identifiable, confidential, or other DOH data/information. Report any suspected confidentiality breech to DOH supervisor/contact. Assure that DOH originated or maintained confidential data/information is not inappropriately retained and returned to the program upon completion of work with DOH program.
OIRM Information Resource Directory Administrator	Use the Information Resource Directory to document confidentiality status of databases, tables, files, elements, and other information as communicated and defined by the Office/Program Manager/Supervisor.
Human Resources	Maintain signed employee confidentiality acknowledgments and annual updates received from employees in personnel files.

Statement of Acknowledgment
Department of Health Confidentiality Policy and Procedures

As an employee, contractor, volunteer, or federal assignee of the Washington State Department of Health (DOH), I understand that I am responsible for maintaining the confidentiality of any data/information collected, maintained, stored, or analyzed within DOH that I may handle during the course of my employment. Release of any data/information and documents must be in accordance with public disclosure or research laws and policies or other laws and policies controlling specific data/informing. I understand that I will receive information from my supervisor on the specific data/information that is confidential and practices for handling this data/information in my program.

I have received and read the DOH confidentiality policy (17.005) and acknowledge that I understand the policy and the responsibilities delegated to me within. I recognize and respect the confidential nature of any data/information I may have access to during the course of my employment with DOH. I will not at any time, nor in any manner, either directly or indirectly divulge, disclose, release, or communicate any confidential data/information to any third party outside the scope of my position unless authorized under the above mentioned laws and policies. I recognize that maintaining confidentiality includes discussing confidential data/information outside of the workplace.

I understand that if I discuss, release, or otherwise disclose confidential data/information outside of the scope of this policy through any means, I may be subject to disciplinary action which may include termination of employment with DOH.

Employee signature: _____ Date: _____

Please print name:_____

Date received by Human Resources Office _____